Method for exchanging at least one secret initial value between a processing station and a chip card

This invention relates to a method for exchanging at least one secret initial value between a processing station and a chip card, in an initializing step for the chip card.

Such methods have been known for some time and are used in producing chip cards, which are employed today in many areas, e.g. in access control systems or as means of payment, for the purpose of safe operation of the chip cards. The chip card usually comprises an integrated circuit and coupling elements electrically connected with the integrated circuit and used for communication with external devices, for example a processing station. The coupling elements are designed either in the form of contact surfaces for touch contacting or as coils for non-touch contacting.

In conventional methods the last step performed in producing the chip card is initialization and personalization of the chip card. This provides the software preconditions for loading all data required for later operation of the card into the memory of the integrated circuit. During initialization all globally necessary data are transmitted for this purpose and the necessary file structures set up. During personalization the individual data are transmitted from the processing station to the chip card and stored in corresponding memory spaces. The data needed for personalization can be for example the name, address and a secret key.

To ensure that the personalizing data, in particular for example a secret key, cannot be intercepted during personalization to avoid later misuse, initialization and personalization are in the known method usually performed in separate process steps and sometimes also in separate rooms with different personnel. During initialization a serial number stored on the chip card is for example transmitted for this purpose to the processing station. For transmission the processing station has a terminal. Furthermore the processing station usually has a security module to which the terminal passes on the number of the chip card. In the security module a key is generated with the number of the chip card, the key being transmitted to the chip card by means of the terminal.

In the following personalizing step, data from a data base containing the data necessary for personalization are transmitted to the chip card and stored in the corresponding memory spaces of the chip card. The personalizing data of the personalizing data base are usually present in encrypted form. In order to avoid misuse, the key for decrypting the personalizing data is normally not known to the manufacturer of the chip card. This key is known only to the institute making the personalizing data available, for example a bank issuing the chip card to be used as a means of payment. For further processing of the encrypted personalizing data, they are loaded into the security module of the processing station. The security module offers a separate unit which is specially protected against attempts at manipulation. The security module contains the key needed for decrypting the personalizing data. With this key the personalizing data are decrypted in the security module and then encrypted again with the key generated during initialization, which was previously loaded into the chip card from the security module. The thus encrypted data are transmitted to the chip card from the security module via the terminal. Subsequently the encrypted data are decrypted with the known key in the chip card and stored in the corresponding memory spaces of the integrated circuit of the chip card.

The known method thus has the disadvantage that at least at one time, namely during initialization of the chip card, a secret key needed for data transmission between a processing station and a chip card must be transmitted once in plaintext. If this key is intercepted, all data and secret keys transmitted in the later personalizing step can be decrypted. If the key is individual to a card, at least the security of this one card would be broken.

The problem of the present invention is therefore to state a method for exchanging at least one secret initial value between a processing station and a chip card, during initialization of the chip card, which has greater security and can be used more simply compared to the prior art.

This problem is solved by the features of claim 1.

The invention starts out from the idea of not transmitting sensitive data between the processing station and the chip card in plaintext at any time. This is obtained by generating values both in the processing station and in the chip card which

are transmitted to the chip card or processing station only in part. The secret data are then determined from the generated and the transmitted values both in the chip card and in the processing station.

The special advantage of the invention is that secret data need not be transmitted between processing station and chip card in plaintext at any time during initialization or a subsequent personalizing step. This firstly increases the security of the initializing and personalizing step, and secondly simplifies initialization and personalization because the latter need no longer be performed in separate steps. The resulting reduction in necessary security effort also reduces expenditures in chip card production.

Further advantages of the present invention can be found in the dependent claims and the following description with reference to a figure.

The single figure shows a processing station and a chip card during initialization or personalization of the chip card.

The figure shows processing station *S*, chip card *CC* and data base *DB*. Processing station *S* contains terminal *T* effecting data exchange with chip card *CC*, and security module *HSM* serving to process secret data. These secret data can come for example from data base *DB*. The figure also shows initializing step *IS* and personalizing step *PS*.

When new chip card *CC* is brought in connection with terminal *T* of processing station *S* for initialization, the authenticity of chip card *CC* can first be checked. This is necessary in order to prevent unauthorized chip cards from being initialized and thus obtaining secret data. To check the authenticity of chip card *CC* one can check for example whether the integrated circuit present on the chip card can be assigned to a certain manufacturer. Additionally one can check a serial number generated during production of the integrated circuit. For this purpose the serial number of the integrated circuit located on chip card *CC* is read out via terminal *T*. The thus determined serial number of the integrated circuit of chip card *CC* is then checked for permissibility in security module *HSM*. For this purpose a list of serial numbers stored in data base *DB* is checked.

After the authenticity check, values serving to determine a secret initial value are generated in security module *HSM*, the secret initial value being identical in security module *HSM* and chip card *CC* without the secret initial value being transmitted in plaintext from security module *HSM* via terminal *T* to chip card *CC*. Parts of the values generated in security module *HSM* are transmitted via terminal *T* to chip card *CC*. In chip card *CC* further values for determining the secret initial value are generated, parts of which are in turn transmitted to processing station *S* via terminal *T*. The secret initial value is subsequently determined in the processing station, i.e. in security module *HSM*, from the values generated in security module *HSM* and the values transmitted from the chip card. In chip card *CC* the secret initial value is determined by means of the values generated in the chip card and the values transmitted from the processing station.

The secret initial value can be for example a start value for generating random numbers. The secret initial value can also be used as a secret key for encrypting and decrypting data.

If the secret initial value is used as a key, personalizing data containing further secret keys, among other things, can for example be transmitted to chip card *CC* in a following processing step.

The secret initial value can be generated from the values generated in security module *HSM* and in chip card *CC* for example by means of algorithms or functions. It is especially advantageous if the same function is used for generating the secret initial value both in security module *HSM* and in chip card *CC*. For this purpose the figure provides a function for initializing step *IS* which involves exponentiating a first variable or a first value with a second value and forming a modulo residue to a third value. In security module *HSM* the values g, n and x are generated. Value n is a large prime number, value g a primitive number, i.e. all numbers 1 .... n-1 can be represented in the form g^i mod n. To increase security one should ensure that the value $(n-1)/2$ is likewise a prime number. Value x also generated in security module *HSM* is a random number, for which $x < n$ holds. By means of the function

$$(1) \quad X = g^x \bmod n$$

values g, n and X are processed. Subsequently values g, n and X are transmitted via terminal T to chip card CC. Value x is kept secret in the security module. Value Y is generated in the chip card by means of a further function

$$(2) \quad Y = g^y \bmod n.$$

For this purpose one uses values g and n transmitted from the processing station and value y generated in the chip card. For value y it holds that $y < n$. Value y is a random number which is generated in particular in accordance with an individual identifier of chip card CC, e.g. a serial number. Value y is kept secret in chip card CC, whereas value Y is transmitted to processing station S. In processing station S the secret initial value, which is used as a key, is generated in security module HSM by means of a function

$$(3) \quad K = Y^x \bmod n.$$

The same secret initial value K is generated in chip card CC

$$(4) \quad K = X^y \bmod n.$$

The identity of secret initial value K in chip card CC and security module HSM is ensured since due to the exchange of the values between chip card CC and security module HSM it holds for K that:

$$(5) \quad K = g^{xy} \bmod n.$$

By means of secret key K now present both in security module HSM and in chip card CC the safe transmission of secret personalizing data can be performed in following personalizing step PS. For this purpose personalizing data PD_{KM} encrypted with major key KM are transmitted from data base DB to security module HSM. Major key KM is present in security module HSM and is used for decoding personalizing data PD_{KM}. Personalizing data PD now present in plaintext are encrypted again in a further step. Secret key K is used for this purpose. Thus generated en-

crypted personalizing data PD_K are transmitted via terminal T to chip card CC where they are decoded with secret key K likewise present.

At the end of personalizing step PS secret key K can be deleted both in the chip card and in security module HSM since for further communication between processing station S and chip card CC one can use for example the secret keys contained in personalizing data PD.

Initializing and personalizing steps of the above-described kind can be used not only in the production of chip cards as mentioned at the outset, but also for later extension of chip cards, for example to extend a chip card subsequently by further applications. A chip card hitherto configured only as a credit card can be extended e.g. by an access control application.